AMENDMENTS TO THE CLAIMS

Please amend the claims of the present application as set forth below. In accordance with the PTO's revised amendment format, a detailed listing of all claims has been provided. A status identifier is provided for each claim in a parenthetical expression following each claim number. Changes to the claims are shown by strikethrough (for deleted matter) or underlining (for added matter).

Claims 1—19 were originally filed.

Claims 1, 7 and 17 are currently amended.

Claim 2 was canceled.

No claims are added.

Accordingly, claims 1 and 3—19 are pending.

1.   (Currently Amended.) A system for porting user data from one computer to another, comprising:

a profile carrier, removably connectable to a computer, comprising:

a memory device to store the user data; [[and]]

a smart card associated with a user that alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when one of the memory device or smart card is absent[[.]]; and

wherein the memory device stores a user's profile that can be used for computer configuration.

2.   (Cancelled.)

3.   (Original.) An assembly as recited in claim 1, wherein the smart card stores a passcode and access to the user data in the memory device is enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card.

4.   (Original.) An assembly as recited in claim 1, wherein the memory device stores a public key and the smart card stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated.

5.   (Original.) A profile carrier comprising:

a smart card to store a passcode and a private key from a private/public key pair;

a memory device to store a user profile and a public key from the private/public key pair;

wherein when the smart card and the memory device are interfaced with a common computing unit, the smart card is configured to permit use of the private key following validation of a user-entered passcode with the stored passcode and to authenticate the public key stored on the memory device using the private key; the profile carrier being configured to permit access to the user profile stored on the memory device upon successful authentication of the public key at the smart card.

6.   (Original.) A computer system, comprising:

a computing unit having a memory drive and a smart card reader; and

the profile carrier as recited in claim 5, wherein the memory device is interfaced with the computing unit via the memory drive and the smart card is interfaced with the computing unit via the smart card reader.

7.   (Currently Amended.) A computer system, comprising:

a computer having an interface; and

a profile carrier adapted to use the interface, the profile carrier comprising a smart card associated with a user and a memory device having data memory to store ~~user data~~ a user's profile, wherein the smart card alternately enables access to the ~~user data~~ user's profile when present and disables access to the ~~user data~~ user's profile when absent.

8.   (Original.) A computer system as recited in claim 7, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user data.

9.   (Original.) A computer system as recited in claim 7, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

10. (Original.) A computer system as recited in claim 7, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.

11. (Original.) A computer system, comprising:

a computer having a memory drive and a card reader;

a portable profile carrier to port a user's profile for configuration of the computer, the profile carrier comprising:

(a) an integrated circuit (IC) card associated with the user that can be interfaced with the computer via the card reader; and

(b) a memory device to store the user's profile, the memory device being interfaced with the computer via the memory drive, the IC card enabling access to the user data on the memory device; and

wherein when the profile carrier is interfaced with the computer, the user's profile is accessible to configure the computer.

12.   (Original.) A computer system as recited in claim 11, wherein the IC card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile.

13.   (Original.) A computer system as recited in claim 11, wherein:

the IC card stores a first key;

the memory device stores a second key that is associated with the first key; and

the IC card is configured to authenticate the second key passed in from the memory device using the first key as a condition for enabling access to the user's profile.

14.   (Original.) A computer system as recited in claim 11, wherein:

the IC card stores a passcode and a private key of a public/private key pair;

the memory device stores a public key of the public/private key pair; and

the IC card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key passed in from the memory device using the private key as a condition for enabling access to the user's profile.

15.   (Original.)   A method for porting a user profile for a computer, comprising:

storing a user profile in memory of a smart card secured profile carrier, the smart card secured profile carrier having a smart card that selectively enables access to the user profile in the memory;

interfacing the smart card secured profile carrier with the computer; and

reading the user profile from the memory for use in configuring the computer.

16.   (Original.)   A method as recited in claim 15, further comprising interfacing the smart card secured profile carrier with a different second computer and reading the user profile from the memory for use in configuring the second computer.

17.   (Currently Amended.)   A method comprising:

storing user data and a public key on a portable memory device;

storing ~~access credentials~~ a private key on a smart card, ~~the access credentials enabling access to the user data stored on the portable memory device~~; ~~and~~

interfacing the smart card and the portable memory device with a computer;

~~reading the access credentials from the smart card to enable~~ verifying compatibility of the public key and the private key; and

allowing, in response to the verified compatibility, access to the user data on the portable memory device.

18.   (Original.) A method comprising:

storing user data in a portable memory device;

storing a device-resident key in the memory device;

storing a card-resident key on the smart card, the card-resident key corresponding to the device-resident key;

storing a passcode on the smart card;

interfacing the smart card with a computer;

interfacing the portable memory device with the computer;

receiving a user-entered passcode;

permitting use of the card-resident key following validation of the user-entered passcode with the passcode stored on the smart card;

passing the device-resident key from the memory device to the smart card;

authenticating, at the smart card, the device-resident key using the card-resident key; and

permitting access to the user data stored in the memory device upon successful authentication of the device-resident key.

19.   (Original.) In a system having a computer and a smart card secured profile carrier, the smart card secured profile carrier having memory to store a user profile and a smart card separate from the memory, computer-readable media resident on the profile carrier having executable instructions comprising:

receiving a user-supplied passcode from the computer;

authenticating the user-supplied passcode with a passcode stored on the smart card;

enabling access to a private key on the smart card upon successful authentication of the user-supplied passcode;

receiving a public key from the memory;

authenticating the public key using the private key; and

enabling access to the user profile in the memory upon successful authentication of the public key.